Environmental Law Division Notes

The Environmental Law Division (ELD), United States Army Legal Services Agency, produces the Environmental Law Division Bulletin, which is designed to inform Army environmental law practitioners about current developments in environmental law. The ELD distributes its bulletin electronically in the environmental files area of the Legal Automated Army-Wide Systems Bulletin Board Service. The latest issues, volume 6, numbers 2 and 3, are reproduced in part below.

Fourth Circuit Looks at NEPA Cost Benefit Analysis

In a recent decision, *Hughes River Watershed Conservancy v. Johnson*,[1] the Fourth Circuit Court of Appeals looked at the adequacy of a cost and benefit analysis in an environmental impact statement (EIS). The case provides guidance on the level of detail that is required for economic benefit information in an environmental analysis prepared under National Environmental Policy Act of 1969 (NEPA).[2]

In this case, federal agencies prepared an EIS for construction of a dam in West Virginia. That EIS came under scrutiny in a 1996 decision, *Hughes River Watershed Conservancy v. Glickman*.[3] In *Glickman*, the plaintiffs asserted that the agencies had not provided fair consideration of the project's adverse environmental effects because they had overestimated the economic benefits to be gained from the dam's recreational use. The court of appeals disagreed and determined that the agencies had not violated NEPA.[4] The court remanded this case for the agencies to reevaluate their estimates of recreational benefits. Subsequent EIS analysis was to be based upon net benefits, rather than gross benefits.[5]

The federal agencies obtained a new economic study of the project. This study evaluated all additional recreational benefits provided by the proposed dam and changes in activity mix, and also considered non-use values. The study showed an overall positive benefit-cost ratio for the dam, which supported the project's economic feasibility. The agencies incorporated the study's conclusions into a supplemental EIS, which was again challenged.[6]

In *Hughes River Watershed Conservancy v. Johnson*, the court reviewed Supreme Court cases that addressed NEPA analyses of economic issues. It concluded that an agency is first vested with discretion to determine that certain values–such as recreation–outweigh environmental costs.[7] The court also determined that NEPA requires agencies to balance a project's economic benefits against its environmental effects.[8] Although an agency could choose to go forward with a project that does not make economic sense, it must nevertheless take a "hard look" at the issue.

Looking at the supplemental EIS, the court found that the federal agencies, "in making their economic recreational benefits determinations, considered the total number of visitors to the [p]roject, the number of visitors who would be diverted to the [p]roject from existing facilities, the consumer surplus figure, and non-use values."[9] Such a non-use value would include the value that a person places on knowing the river exists in its free-flowing state and knowing the river will be protected for future generations. The agencies' weighing of these factors led the court to determine that the agencies' decision to implement the project was not arbitrary or capricious.[10]

This case demonstrates that economic benefit information in a NEPA document must be thorough and even-handed. The

1. 165 F.3d 283 (4th Cir. 1999).
2. 42 U.S.C.A. § 4321 (West 1999).
3. 81 F.3d 437 (4th Cir. 1996).
4. *Id.* at 447.
5. *Id.*
6. *Johnson*, 165 F.3d at 287.
7. *Id.* at 288 (citing Marsh v. Oregon Natural Resources Council, 490 U.S. 360, 378 (1989)).
8. *Id.* at 289 (citing Robertson v. Methow Valley Citizens Council, 490 U.S. 332, 349 (1989)).
9. *Id.* at 290.
10. *Id*.

fact that certain factors are imprecise or unquantifiable will not render the result inadequate.[11] Lieutenant Colonel Howlett.

EPA Proposes New Rules for Lead-Based Paint Debris

The Environmental Protection Agency (EPA) has proposed a new rule on lead-based paint (LBP) demolition debris.[12] Under the latest proposal, LBP demolition debris that fails the toxicity characteristic leaching procedure would no longer be subject to regulation under the Resource Conservation and Recovery Act (RCRA).[13] The trade-off, however, is that all LBP demolition debris, regardless of the hazard, would be subject to regulation under the Toxic Substances Control Act (TSCA).[14]

The TSCA regime would require that: (1) the LBP debris be stored for up to 180 days in an inaccessible container (or seventy-two hours if it is accessible), (2) the LBP debris be disposed in construction/demolition waste landfills (not municipal landfills) or hazardous waste disposal facilities, and (3) disposal facilities be notified that the waste that contains LBP demolition debris with information on the date the debris was generated. The generator and the landfill would have to keep records for three years.[15]

The proposed rule includes a household waste exemption.[16] Accordingly, wastes from a resident's home renovations would not be included in the rule's purview.[17] The Army, as the executive agent, is currently coordinating comments from all of the services for a single DOD submittal. Major Egan.

ELD Fines and Settlements Report

In January, the ELD published its *Fines and Settlements Report* for the first quarter of fiscal year 1999.[18] This report indicated that Army installations received two new fines and settled seven cases during the quarter. In addition, for the first time, the report deemed five other cases closed because states failed to pursue fines after installations raised a sovereign immunity defense.

Each of the sovereign immunity cases deemed closed in the *ELD Quarterly Fines and Settlements Report* involved asserted violations of the Clean Air Act (CAA).[19] Sovereign immunity has been waived for CAA enforcement by state regulators, but not for payment of state punitive fines.[20] In each of the closed cases discussed in the ELD's report, Army installations had invoked sovereign immunity under the CAA, and heard nothing further from their respective state regulators.

The decision to close these pending cases was made on an individual basis. Accordingly, it does not mean that all cases involving sovereign immunity are deemed resolved. The decision to close each case was made on a variety of factors. Such factors include the length of time that has passed since the violation, the lack of contact from the state, and the likelihood that the state will revive the action in the future.

A number of installations are currently facing uncertainty in determining closure for specific cases that may involve sovereign immunity. In most of these cases, the installation sent a letter to the state regulators informing them that sovereign immunity precludes payment of fines. In each case, the states have simply not responded to the letters. In general, the best practice under these circumstances is to maintain contact with state officials and attempt to receive official acknowledgment (by letter, motion, or otherwise) that the fine is no longer pending.

In some cases, however, it may be wise to "let sleeping dogs lie." Over time, the failure of the state regulators to pursue an outstanding notice of violation may be deemed acquiescence to

---

11. *Id*. (quoting Sierra Club v. Lynn, 502 F.2d 43, 61 (5th Cir. 1974)).

12. Temporary Suspension of Toxicity Characteristic Rule for Specified Lead-Based Paint Debris, Part II, 63 Fed. Reg. 70,233 (Dec. 18, 1998).

13. 42 U.S.C.A. § 6900 (West 1999).

14. 63 Fed. Reg. 70233, 70235.

15. Temporary Suspension of Toxicity Characteristic Rule for Specified Lead-Based Paint Debris, Part II, 63 Fed. Reg. at 70,235.

16. *Id.* at 70,241.

17. *Id.* at 70,241-42.

18. Environmental Law Division, U.S. Army Legal Services Agency, Quarterly Fines and Settlements Report (1st quarter, 1999). For a copy of this report, please contact the author at <cotelrj@hqda.army.mil>.

19. 42 U.S.C.A. §§ 7401-7671q (West 1999).

20. The Supreme Court first articulated this view in *United States Department of Energy v. Ohio*, where it interpreted a congressional waiver of sovereign immunity for the Clean Water Act (CWA), which was similar to the CAA. *See* United States Dep't of Energy v. Ohio, 503 U.S. 607 (1992) (citing 33 U.S.C.A. § 1251-1277 (West 1999)). The Supreme Court's decision was formally extended to the CAA in *United States v. Georgia Department of Natural Resources. See* United States v. Georgia Dep't of Natural Resources, 897 F. Supp. 1464 (N.D. Ga. 1995).

the United States' position on sovereign immunity. Major Cotell.

Invoking Sovereign Immunity in Clean Air Act Issues

As the previous note discussed, states have failed to close CAA cases that are pending against installations–even though the installations have raised the sovereign immunity defense. The reasons for this varies. Some states are unfamiliar with the concept of sovereign immunity, believing that dismissal of a case will somehow affect their "rights." Others believe that they may be able to resurrect an action if the CAA cases that are currently under appeal are decided in their favor. There is some truth to these assertions.

One invalid reason that states keep cases open, however, results from the installation's failure to adequately explain the scope of sovereign immunity. Once a state is told that the federal government is invoking "immunity" from state action, some regulators experience undue panic. Often, states incorrectly jump to the conclusion that they are powerless to regulate an installation.[21] This issue becomes particularly dangerous when state regulators believe that their only regulatory recourse is to deny CAA permits after an installation invokes sovereign immunity.

Accordingly, it is important for the installation environmental law specialist (ELS) to adequately explain the sovereign immunity issue when an installation receives a CAA notice of violation from a state regulator. The ELS should stress to the regulator that, under the CAA, sovereign immunity applies only to the imposition of fines. In all other areas of the CAA, immunity has been waived. States may require corrective action and other measures to compel immediate compliance. It is in the best interest of the installation to acknowledge these requirements and express a willingness to cooperate. In addition, it is important to note that the installation is powerless to effect a waiver of sovereign immunity. This power rests only with Congress. Accordingly, a diplomatic letter can express to the state that this issue is beyond an installation's control. This will likely have a positive effect on future dialogue with the regulators. Attached as an appendix to this note is a sample letter that should be used by installations to invoke sovereign immunity. Obviously, the letter must be tailored by each installation to address the specifics of its case. Major Cotell.

21. One recent case required a detailed letter from the Department of Defense Deputy General Counsel (Installations and Environment) explaining the concept of sovereign immunity to state regulators and addressing their erroneous assumptions about the immunity's scope.

Sample Letter to State Regulators Invoking Sovereign Immunity for Cases Concerning the Clean Air Act

Date

Address of state regulatory agency

Dear _____,

This is in response to a Notice of Violation (NOV) issued from your office on (***date***) to (***Installation***) for violations of (***cite state reference)*** pursuant to the Clean Air Act (CAA) and for demand of a fine in the amount of (***amount***).

The (***Installation***) takes very seriously its obligation to maintain compliance with environmental laws and regulations. In the area of environmental law, Congress has frequently waived sovereign immunity to require federal agencies to comply with state, interstate, and local pollution control laws. Indeed, the CAA's federal facilities provision (42 U.S.C Section 7418(a)) contains a partial waiver of sovereign immunity that directs federal agencies to comply with air pollution control programs "to the same extent as any non-governmental entity." In addition, it subjects federal facilities to administrative fees or charges to defray the costs of air pollution control programs, as well as the "process and sanctions" of air program regulatory agencies.

In light of the above, to the extent that (***Installation***) has violated the CAA, it has a duty and obligation to correct the deficiencies expeditiously and in accordance with all applicable state laws. The violations in the above noted NOV are being handled by (***Director of Installation Environmental Program***) and specific action is being taken to bring (***Installation***) into immediate compliance and to correct deficiencies.

Please note that although the waiver of sovereign immunity in the CAA includes subjecting federal facilities to "process and sanctions," the precise meaning of these words has been the subject of litigation in federal courts. Indeed, the position of the United States taken in pending litigation on this matter will prevent (***Installation***) from paying the fines requested in the NOV in this case. The terms "process and sanctions" were first interpreted by the United States Supreme Court when it examined the federal facilities provision of the Clean Water Act (CWA) in U.S. Department of Energy v. Ohio, 503 U.S. 607 (1992). The Court found that this aspect of the CWA's waiver of sovereign immunity, which is virtually identical to the waiver in the CAA, did not subject federal facilities to "punitive fines" imposed as a penalty for past violations. This was based on a finding that the CWA did not contain a clear and unequivocal congressional waiver of sovereign immunity on that point.

The Supreme Court's decision in Department of Energy v. Ohio was formally extended to the CAA in United States v. Georgia Department of Natural Resources, 897 F. Supp. 1464 (N.D. Ga. 1995), holding that the CAA does not authorize Federal agencies to pay punitive fines. More recently, a federal district court in California similarly held that the CAA does not authorize federal agencies to pay punitive fines. Sacramento Metropolitan Air Quality Control District v. United States, 29 F. Supp. 652 (E.D. Cal. 1998). Although a contrary result was reached in another federal court case where a district court judge deviated from the model analytical approach of the U.S. Supreme Court, that case is currently pending appeal before the Federal Court of Appeals for the 6th Circuit. United States v. Tennessee Air Pollution Control Board, 967 F. Supp. 975 (M.D. Tenn. 1997), *appeal pending*, No. 97-5715 (6th Cir.). The position of the United States, as articulated by the Department of Justice in defense of litigation on this matter, is that Congress has not waived sovereign immunity under the CAA for the payment of punitive fines imposed by states.

(***Installation***) is bound by this position. No individual installation may waive sovereign immunity. Indeed, not even an agency such as the Army or the Department of Defense may waive sovereign immunity. Only Congress has that power, and, until Congress exercises it, (***Installation***) cannot legally pay the fines requested in the NOV.

The lack of a waiver of sovereign immunity for punitive fines in no way exempts federal agencies from full compliance with the CAA. Federal agencies are bound to comply with all laws and regulations for air pollution control, and are subject to payment of administrative fees and any court-imposed coercive fines. Where deficiencies are noted in a federal facility's air pollution control activities, the facility has the same obligation as non-governmental entities to expeditiously correct all infractions. Again, (***Installation***) remains firmly committed to environmental compliance and will work closely with your agency to assure all compliance issues related to this matter are quickly resolved.

Sincerely,

Installation Commander/Staff Judge Advocate

Puerto Rican Case Explores CERCLA Jurisdictional Limit

A recent case[22] in the Federal District Court in Puerto Rico explores the jurisdictional limits of section 113(h) of the Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA).[23] In *M.R. (VEGA ALTA), Inc. v. Caribe General Electric Products, Inc.*, the plaintiffs sued both private defendants and the United States EPA, alleging that these parties were responsible for solvent contamination in plaintiffs' water supply.[24] In addition to bringing CERCLA claims, and a variety of tort claims, against private defendants, the plaintiffs also used CERCLA's citizen suit provision, to challenge the EPA.[25] This precedent is important to because the Army has been delegated the same authority that the EPA exercised in this case.[26]

In 1988, the EPA ordered the private defendants to implement a remedial action. The EPA modified its remedial approach several times over the next ten years, although the remedial action was still underway. The plaintiffs brought suit to compel the private defendants to carry out the agency's remediation order under CERCLA's citizen suit provision, CERCLA section 310(a)(1). In addition, the plaintiffs sued the EPA under CERCLA section 310(a)(2), alleging that the EPA: (1) had not selected an adequate remedy, (2) had not implemented selected remedies, and (3) had failed to perform required five-year reviews.[27] The plaintiffs also sued the EPA under the Administrative Procedure Act.[28]

The court began its discussion of the citizens' suit claims by stressing that CERCLA's grant of federal jurisdiction is limited by CERCLA section 113(h).[29] As for the claim against the private defendants, the court found that it was allowable since that claim sought to enforce an EPA order issued under CERCLA section 106.[30] Regarding the claim against the EPA, the district court began by examining CERCLA's legislative history. The court determined that, according to CERCLA section 113(h)(4), it had no jurisdiction over the plaintiffs' challenge to an ongoing response stating:action. The court stated:

> Plaintiffs wish to require the EPA immediately to (1) initiate control of soil contamination by use of certain technologies, (2) initiate extraction and treatment of contaminated groundwater, and (3) conduct and act upon the findings of a remedy review. In order to provide this type of relief, we could not avoid interfering with the EPA's cleanup efforts and running afoul of the mandate of section 113(h).[31]

The court also found that the Administrative Procedure Act claim was barred since CERCLA section 113(h) refers to "any

---

22. M.R. (VEGA ALTA), Inc. v. Caribe Gen. Elec. Prods., Inc., 31 F. Supp. 2d 226 (D.P.R. 1998).

23. 42 U.S.C.A. §§ 9601-9675 (West 1999).

24. Plaintiffs were represented by Ms. Margaret Strand, a Washington, D.C., practitioner, who is familiar to many Army lawyers through her educational activities.

25. CERCLA § 310(a)(1) (codified at 42 U.S.C.A. § 9659(a)(1)). This note does not discuss the private defendant claims or the Federal Tort Claims Act count against the EPA.

26. *See* Exec. Order No. 12580, 52 Fed. Reg. 2923 (1987).

27. The EPA is required to review all remedial actions that result in hazardous substances remaining on the site no less than every five years after the remedial action is initiated. Such review is meant to assure that human health and the environment are being protected by the remedial action being implemented. 42 U.S.C.A. § 9621(c). *See* 40 C.F.R. § 300.430(f)(4)(ii) (1998).

28. 5 U.S.C.A. § 706 (West 1999).

29. 42 U.S.C.A. § 9613(h). This section states:

No Federal court shall have jurisdiction under Federal Law . . . to review any challenges to removal or remedial action . . ., or to review any order . . . , in any action except one of the following:

> (1) An action under section 9607 of this title [CERCLA] to recover response costs or damages or for contribution.
> (2) An action to enforce an order issued under section 9606(a) of this title or to recover a penalty for violation of such order.
> (3) An action for reimbursement under section 9606(b)(2) of this title.
> (4) An action under section 9659 of this title (relating to citizens suits) alleging that the removal or remedial action taken under section 9604 of this title or secured under section 9606 of this title was in violation of any requirement of this [Act]. Such an action may not be brought with regard to a removal where a remedial action is to be undertaken at the site.

An action under section 9606 of this title in which the United States has moved to compel a remedial action.

Id.

30. *See id.*

31. M.R. (VEGA ALTA), Inc. v. Caribe Gen. Elec. Prods., Inc., 31 F. Supp. 2d 226, 235 (D.P.R. 1998).

challenges" to a removal action(not just those that are brought under CERCLA.[32]

On the other hand, the court found that the request for a five-year review did *not* constitute a challenge to the ongoing response action. On this matter, the court stated that "[r]equiring the EPA to produce a five-year review in accordance with CERCLA § 121(c), 42 U.S.C. § 9621(c), would not affect the remedial action or unduly compromise the EPA's limited resources, in contravention of congressional policy behind section 113(h)."[33]

Under the logic of this case, a challenge can be brought to compel CERCLA procedural requirements as long as there is no interference with the implementation of the remedy. This could require an inquiry into whether the requested relief interferes with a remedy and is not preferable to a "bright-line" rule that would bar all CERCLA challenges to an ongoing remedy. This decision represents an erosion of CERCLA section 113's protections. Lieutenant Colonel Howlett.

Longhorn Pipeline Settlement Reached

On 5 March 1999, the United States District Court for the Western District of Texas approved a settlement among the parties to the Longhorn Partners Pipeline (LPP) dispute.[34] Originally, the plaintiffs sued to stop the operation of a proposed 700-mile pipeline, claiming that the project violated the requirements of the national Environmental Policy Act.[35] The suit named several federal defendats: the Army, the EPA, the Department of Transportation (DOT), and the Federal Energy Commission. Among other things, the plaintiff's alleged that the Army's involvement inthe case stemmed from an LPP application for a six-mile right-of-way across Fort Bliss, Texas, and from actions by the plaintiffs that fell within the jurisdiction of the Army Corps of Engineers.

The District Court granted the injunction in August 1998 and ordered the EPA "and/or" DOT to prepare an Environmental Impact Statement addressing the construction and operation of the pipeline. Under the terms of the settlement, the plaintiffs have agreed to accept preparation of an Enviornmental Assessment (EA) by EPA and DOT. This EA will include an analysis of the affected enviornment and a consideration of alternatives to construction (such as -re-rerouting the pipeline around environmentally sensitive areas), as well as alternative measure to mitigate any identified impacts. The EPA and DOT expect the EA to be completed in a seven-month period. The Army will be a cooperating agency under the agreement. Major DeRoma.

Litigation Division Note

Y2K Legal and Litigation Issues

Introduction

By now, anyone who is not aware of the Year 2000 computer problem, known as "Y2K," has been living in a cave. Some of the more paranoid commentators predict that the Y2K bug will spawn a worldwide depression or recession, resulting in riots, blackouts, looting, food shortages, and violence.[36] This has created a cottage industry for firms catering to survivalists. In preparation for the millennium, these firms are selling the public such items as freeze-dried food, alternate energy sources, and weapons.[37] Many fear that, after the dust settles and the fires are extinguished, lawyers will move in like vultures to feast on the remains of civilization. Some predict the litigation fallout from Y2K to be the next asbestos or tobacco. Whether one thinks that Y2K is the next apocalypse or the biggest "non-event" of the century, prudence dictates that judge advocates prepare their clients for the potential legal issues stemming from the Y2K bug. This note is not an in-depth analysis of the legal issues involved; rather, it provides an overview of the Y2K problem, the remediation efforts underway in the Army and the Department of Defense (DOD), and the potential legal issues involved.

---

32. *Id*. (quoting McClellan Ecological Seepage Situation v. Perry, 47 F.3d 325, 329 (9th Cir. 1995)).

33. *Id*.

34. Spiller v. Walker, No. A-98-CA-255-SS (W.D. Tx. Mar. 5, 1999).

35. 42 U.S.C.A. §§ 4321-4370d (West 1999).

36. *See* James K. Glassman, *Bonkers Over Y2K*, WASH. POST, Dec. 1, 1998, at A25.

37. *See id*. *See also Real-World Contingency Plan* (visited Mar. 24, 99) <http://www.y2knewswire.com/plan.htm>.

The Source and Scope of the Problem

Over the past several decades, computer programmers have written software and designed computer systems using two digit numbers to represent dates (for example, a computer would store 1998 as "98"). This practice increased processing capabilities and saved expensive memory space within the systems. Unfortunately, it also resulted in systems that are unable to distinguish the year 2000 from the year 1900, 2001 from 1901, and so on.[38] On the stroke of midnight, 1 January 2000, these systems may malfunction or completely shut down. Operational and strategic military systems, telecommunications, pay and finance, personnel systems, security systems, weapons systems, and a myriad of other functions that are dependent on computers could fail and disrupt military operations.[39]

The problem, however, goes far beyond computers. Many electronic devices contain internal processors (often referred to as "embedded chips") that may also fail or malfunction on 1 January 2000. The failure of these embedded chips could also disrupt normal operations for days, shutting down traffic lights, elevators, heating and air-conditioning systems, medical devices, security locks, and fire alarms.[40]

Just how big is the problem? The White House Office of Management and Budget currently estimates that it will cost the federal government $6.8 billion to fix its most important computers.[41] Within the DOD, the cost to repair the mission-critical systems for Fiscal Years (FY) 1996-2000 was $2.61 billion, with an estimated $1.92 million in FY 2001 costs.[42] As of 31 December 1998, eighty-one percent of the DOD's mission-critical systems were validated as being Y2K-compliant, with an anticipated ninety-three percent fix by 31 March 1999.[43] Nevertheless, Congress has expressed serious concerns regarding the DOD's Y2K remediation progress.[44]

The Army's figures are similar. As of 15 October 1998, the Army had 638 mission-critical systems, seventy-six percent of which were Y2K compliant.[45] More than ninety-four percent of the Army's weapons systems are compliant.[46] There are also over 13,900 non-mission-critical Army information systems and 444,196 information technology (IT)-controlled devices throughout the Army. The Army estimates that there are 6740 weapon and automation systems, which must be repaired, at a projected cost of $233 million. Additionally, the Army estimates that there are 153,445 infrastructure devices with the Y2K problem, with a projected repair cost of $126 million.[47] Fortunately, the Army has a systematic plan for identifying and

---

38. UNITED STATES GENERAL ACCOUNTING OFF., DEFENSE COMPUTERS: YEAR 2000 COMPUTER PROBLEMS THREATEN DOD OPERATIONS, GAO/AIMD-98-72, B-278156 (Apr. 30, 1998) at 5-6.

39. *Id*. at 5-7.

40. *Id*. at 6. *See also* Miriam F. Browning, *Winning the First War of the Information Age: Year 2000*, ARMY RD&A, Jan.–Feb. 1999, at 2, 5.

41. UNITED STATES OFF. OF MGMT. AND BUDGET, 8TH Q. REP.: PROGRESS ON YEAR 2000 CONVERSION, (Mar. 18, 1999), at Executive Summary [hereinafter OMB REP.], *available at* <http://www.cio.gov/8thQuarterlyReport.doc>.

42. *Id.* at app. A, tbl. 1. *See* Stephen Barr, *A Fix in Time to Keep Agencies Running*, WASHINGTON POST, Aug. 3, 1998, at A01 (containing the Army's definition of a "mission-critical system").

43. *Oversight of the Year 2000 Problem at the Department of Defense: How Prepared is our Nation's Defense?*: *Hearing Before the Subcomm. on Government Management, Information, and Technology,* 106th Cong. (1999) (statement of John Hamre, Deputy Secretary Of Defense) [hereinafter Hamre Statement], *available at* <http://www.house.gov/reform/gmit/hearings/testimony/990302jh.htm>. The recent OMB quarterly report, however, indicated that the DOD had only fixed 72 percent (1670 of 2306) of its mission-critical systems. *See* OMB REP., *supra* note 41, at App. A, tbl. 1. The discrepancy in numbers (81% vs. 72%) prompted congressional criticism.

44. Representative Stephen Horn, *The Progress of the Executive Branch in Meeting the Year 2000 (Y2K) Problem* (Feb. 22, 1999), *available at* <http://www.house.gov/reform/gmit/y2k/990222.htm>. Representative Horn, Chairman of the Subcommittee on Government Management, Information, and Technology, House Committee on Government Reform, made the following observation in the latest House assessment of the federal government's Y2K remediation progress:

> Six organizations lowered an otherwise stellar [overall federal government] grade to mediocrity. But together, these agencies–the Departments of Agriculture, Defense, Health and Human Services, State, and Transportation, and the Agency for International Development–are responsible for more than 50 percent of all mission-critical computer systems in the federal government. Our concerns about these agencies are plentiful. For example, last December the Department of Defense reported that 81 percent of its mission-critical systems were Year 2000 compliant. But in the department's quarterly report this month, officials stated that only 72 percent were compliant. Either the department has a serious internal communications problem, or it has taken a very big step backward in its Year 2000 efforts. Either way, the situation is alarming. Today, DOD's biggest battle is fixing its own computer systems.

Id. Representative Horn gave the DOD a grade of a "C-" This was up from a "D-" on 13 November 1998. *See id.*

45. Browning, *supra* note 40, at 3. Mission-critical systems are those major weapon systems and IT systems that "directly affect the Army's go-to-war mission and are necessary for commander-in-chief (CINC) deployments and exercises." *Id*. Examples of mission-critical weapons systems include the Patriot Missile System, the Apache Attack Helicopter, and the Single Channel Ground and Airborne Radio System. Examples of mission-critical IT systems include the Army Total Asset Visibility System and the Standard Depot System. *Id.*

46. *Id*.

repairing noncompliant systems and developing contingency plans to address the potential fallout from Y2K-related systems failures.[48]

Litigation

The repair costs, however, pale in comparison to the estimated litigation costs. Companies in the United States will spend an estimated $300 to $600 billion dollars making their systems Y2K complaint.[49] In addition, some commentators are predicting a "litigation explosion with predicted costs estimated as high as $1.5 *trillion*."[50] The federal government will certainly become involved in many types of litigation, but two types will probably dominate the government's time: contract litigation and tort litigation.

One category of government Y2K litigation will probably involve affirmative claims by the government against contractors that have provided IT that is not Y2K compliant. Since 1997, Part 39 of the Federal Acquisition Regulation (FAR) has required agencies to ensure that IT contracts contain provisions that require the IT to be Y2K compliant.[51] In addition to the FAR provisions, there are also statutory and other constraints on purchasing IT that is not Y2K compliant.[52]

Information technology is Y2K compliant if:

> [It] accurately processes date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations, to the extent that other information technology, used in combination with the information technology being acquired, properly exchanges date/time data with it.[53]

There are, however, two broad limitations to the scope of Part 39. First, it applies only to "information technology," the definition of which expressly excludes embedded chips.[54] Second, a system only has to be compliant "to the extent that other information technology . . . properly exchanges date/time data

47. *Id*. at 3-4. The "infrastructure devices" include communications hardware and software; personal computers and servers; and facilities/infrastructure. *Id*. at 4.

48. *See id*. *See also* Lieutenant General William H. Campbell and Captain Shurman L. Vines, *Year 2000 Operational Evaluations*, ARMY RD&A, Jan.–Feb. 1999, at 7. Lieutenant General Campbell, the Director of Information Systems for Command, Control, Communications and Computers, Headquarters, Department of the Army, designated Y2K as his top priority. *Id*.

49. *See* Glassman, *supra* note 36.

50. Clyde Wilson, *The Year 2000 Litigation Explosion: Prevention, Mitigation and Planning, available at* <http://www.itpolicy.gsa.gov/mks/yr2000/y2kconf/papers/paper23fp.htm>, (visited Mar. 16, 1999) (emphasis added) (citing Warren S. Reid, *The Year 2000 Crisis: What Surprises are Left*, CYBERSPACE LAW., Sept. 1997). *See* Stephen Barr, *Study Says Y2K Risks Widespread*, WASH. POST, Feb. 24, 1999, at A1 (quoting Representative Dreirer, who estimated litigation costs to be $1 trillion.).

51. GENERAL SERVS. ADMIN. ET AL., FEDERAL ACQUISITION REG. 39.106 (June 1997) [hereinafter FAR]. This regulation states:

> 39.106–Year 2000 Compliance
> When acquiring information technology that will be required to perform date/time processing involving dates subsequent to December 31, 1999, agencies shall ensure that solicitations and contracts—
> (a)(1) Require the information technology to be Year 2000 compliant; or
> (2) Require that non-compliant information technology be upgraded to be Year 2000 compliant prior to the earlier of
> (i) The earliest date on which the information technology may be required to perform date/time processing involving dates later than December 31, 1999, or
> (ii) December 31, 1999; and
> (b) As appropriate, describe existing information technology that will be used with the information technology to be acquired and identify whether the existing information technology is Year 2000 compliant.

Id.

52. Strom Thurmond National Defense Authorization Act of Fiscal Year 1999, Pub. L. No. 105-261, § 333(a), 112 Stat. 1920 (1998). The Act states:

> (a) Funds for Completion of Year 2000 Conversion.—None of the funds authorized to be appropriated pursuant to this Act may (except as provided in subsection (b)) be obligated or expended on the development or modernization of any information technology or national security system of the Department of Defense in use by the Department of Defense (whether or not the system is a mission critical system) if the date-related data processing capability of that system does not meet certification level 1a, 1b, or 2 (as prescribed in the April 1997 publication of the Department of Defense entitled "Year 2000 Management Plan").

Id. See Department of Defense Appropriations Act, Pub. L. 105-262, § 8116, 112 Stat. 2279 (1998) (identical provision). The Secretary of Defense has also restricted the use of funds for noncompliant systems. *See also* Memorandum, The Secretary of Defense, subject: Year 2000 Compliance (7 Aug. 1998) (prohibiting the obligation of funds for all mission-critical and IT systems that are not Y2K compliant).

53. FAR, *supra* note 51, at 39.002.

with it."[55] This latter exception could make it difficult for the government to prove that a particular IT system is not Y2K compliant. This difficulty arises because the government may have to first prove that all other IT systems feeding data into the system are compliant.[56]

Once the government has accepted noncompliant IT, its remedies against the contractor will be severely limited, absent "latent defects, fraud, gross mistakes amounting to fraud, or as otherwise provided in the contract."[57] Because of these limitations, much of the litigation regarding noncompliant IT may involve disputes over whether the Y2K defect was a latent or patent defect.[58]

To expand the Army's remedies in the event IT is not compliant, the Office of the Assistant Secretary of the Army for Research, Development, and Acquisition (SARDA) issued a memorandum in October 1997 encouraging contracting officers to incorporate Y2K warranty clauses into IT solicitations.[59] In so doing, the SARDA intended to provide remedies for noncompliant IT that are beyond those contained in standard inspection and acceptance clauses.[60] The additional remedies that are available will depend on the language incorporated into the warranty.

Year 2000-related tort claims may be another potential area of litigation for the government. Under the Federal Tort Claims Act (FTCA), individuals may recover for personal injury, death, or property damage caused by the negligent acts of government employees acting within the scope of their employment.[61] Given the wide range of potential tort suits (and the equally wide range of personal injury attorneys), Y2K-related litigation will likely span the spectrum from traffic accidents to wrongful death suits. One possible area of litigation is personal injury litigation brought on by Y2K-related medical equipment failures. For example, imagine that a noncompliant embedded chip in a heart monitor locks up at midnight on 1 January 2000 and causes the monitor to shut down. The monitor then fails to alert the nurse's station of the patient's heart attack, and the patient subsequently dies. The family later discovers that the hospital staff knew or should have known that the monitor was not

---

54. *Id.* at 2.101. This regulation defines information technology as:

> [A]ny equipment, or interconnected system(s) or subsystem(s) of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.
> (a) For purposes of this definition, equipment is used by an agency if the equipment is used by the agency directly or is used by a contractor under a contract with the agency which–
> (1) Requires the use of such equipment; or
> (2) Requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.
> (b) The term *information technology* includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.
> (c) The term *information technology* does not include–
> (1) Any equipment that is acquired by a contractor incidental to a contract; or
> (2) Any equipment that contains imbedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, HVAC (heating, ventilation, and air conditioning) equipment such as thermostats or temperature control devices, and medical equipment where information technology is integral to its operation, are not information technology.

Id.

55. *Id.* at 39.002.

56. *See* RICHARD O. DUVALL ET AL., YEAR 2000 ISSUES IN GOVERNMENT CONTRACTS 26-27 (1999).

57. FAR, *supra* note 51, at 46.501 ("Acceptance constitutes acknowledgment that the supplies or services conform with applicable contract quality and quantity requirements, except as provided in this subpart and subject to other terms and conditions of the contract."). *See id.* at 52.246-2(k) ("Inspections and tests by the government do not relieve the contractor of responsibility for defects or other failures to meet contract requirements discovered before acceptance. Acceptance shall be conclusive, except for latent defects, fraud, gross mistakes amounting to fraud, or as otherwise provided in the contract."). *See also* JOHN CIBINIC, JR. & RALPH C. NASH, JR., ADMINISTRATION OF GOVERNMENT CONTRACTS 866-99 (3d ed. 1995) (providing a thorough discussion of the effect of final acceptance on the government's rights).

58. A latent defect is "a defect which exists at the time of the acceptance but cannot be discovered by a reasonable inspection." FAR, *supra* note 51, at 46.101. A patent defect is "any defect which exists at the time of acceptance which is not a latent defect." *Id*. *See* DUVALL ET AL., *supra* note 56, at 35-38 (discussing the potential "latent" vs. "patent" defect issue in the Y2K setting).

59. Memorandum, Assistant Secretary of the Army for Research, Development, and Acquisition, subject: Assuring Year 2000 Compliance in Information Technology (IT) Contracts (21 Oct. 1997).

60. *Id*. *See* FAR, *supra* note 51, at 52.246-2(k), 46.501.

61. *See* 28 U.S.C.A. § 1346(b) (West 1999). The law of the state where the act or omission occurred determines the liability of the United States. *Id*. *See also id* § 2672 (providing a thorough discussion of the Federal Tort Claims Act). *See generally* ADMINISTRATIVE & CIVIL L. DEP'T, THE JUDGE ADVOCATE GENERAL'S SCHOOL, U.S. ARMY, JA-241, FEDERAL TORT CLAIMS ACT (May 1997).

Y2K-compliant, and sues the hospital for failing to correct the problem.

What makes this particular area of tort litigation such a concern? Senator Robert F. Bennett, Chairman of the Senate Special Committee on the Year 2000 Technology Problem, recently released a committee report that "singles out health care as the worst-prepared industry for the Y2K glitch."[62] The Senate report cites the pharmaceutical supply chain and medical diagnostic equipment as two major risks within the industry.[63] Claims judge advocates (CJA) can be assured that, according to the Deputy Secretary of Defense, the DOD is far ahead of the rest of the healthcare industry in risk management.[64] Nevertheless, the CJA should determine what Y2K remediation efforts are underway at the local military medical treatment facility.

Finally, there may be some legislative relief on Y2K litigation, although not in the area of personal injury law. Both the House and the Senate are considering versions of the Year 2000 Fairness and Responsibility Act.[65] If it becomes law, the Act would require ninety-day waiting periods for certain Y2K suits, create a duty for plaintiffs to mitigate damages, and limit economic awards to those provided for by contract or incidental to personal injury or property damage claims.[66] The Act would also give federal district courts original jurisdiction over Y2K class action lawsuits.[67] Besides federal efforts, there are over 100 bills in various state legislatures concerning Y2K.[68]

Other Legal Issues

Besides litigation, the Y2K problem may create legal issues in other areas. Criminal investigations and courts-martial may be adversely affected by Y2K-related errors at forensic laboratories. There may be criminal or civil procurement fraud actions against contractors who defraud the government.[69] Legal assistance offices may be inundated with soldiers seeking assistance with pay, credit, and other date-related financial problems.[70] There may be employment actions involving federal civilian employees or contractor employees who failed to take appropriate measures relating toY2K remediation. Failures at chemical sites may cause massive environmental hazards.[71] The most immediate and largest-scale legal issues, however, may come not from within, but from off-post. Specifically, on 1 January 2000 the Army may see a flood of requests for civil assistance from local and state officials.

Many installations have dealt with natural or human disasters that result in time-sensitive requests for support (for example, a heavy winter storm or the bombing of a federal building).[72] Typically, these disasters are localized; however, if the Y2K problem results in disaster-level disruptions, they will strike simultaneously across the nation and the world. This has the potential to greatly stress the ability of the DOD to respond to these emergencies while maintaining operational readiness.[73] To counter these stresses, the Deputy Secretary of Defense has issued specific guidance relating to support to civil authorities for Y2K-related problems.

---

62. United States Senate Special Committee on the Year 2000 Technology Problem, *Investigating the Impact of the Year 2000 Problem*, *available at* <http://www.senate.gov/~y2k/> (explaining that health care in the international community is at high risk for Y2K failures).

63. *Id*.

64. In testimony before the House committee, the Deputy Secretary of Defense stated:

> [Department of Defense] biomedical equipment is currently 96 percent Y2K compliant. The remaining 4 percent will be compliant by March 31, 1999. "Biomedical" means instruments and equipment typically found in a clinic, hospital, doctor's or dentist's office. As an example, some electrocardiogram (EKG) machines have a date function that could be affected by Y2K. The EKG equipment, however, records analog signals that are not date-dependent. Thus, the equipment deals with dates only to tag the data.

Hamre Testimony, *supra* note 43. *See* Lieutenant Colonel James B. Crowther, *The U.S. Army Medical Command's Cure for the Millennium Bug*, ARMY RD&A, Jan.–Feb. 1999, at 13 (providing details on the U.S. Army Medical Command's Y2K efforts). *See also* The Tri-Service Infrastructure Program Office Year 2000 Knowledge Center (visited 29 Mar. 1999), *available at* <http://www.timpo.osd.mil/y2k/>.

65. *See* H.R. 775, 106th Cong., (1999) *available at* <http://www.ogc.doc.gov/ogc/fl/cld/hi/hr775.html>; S. 461, 106th Cong. (1999), *available at* <http://www.ogc.doc.gov/ogc/fl/cld/hi/s461.html>.

66. *See* Martha L. Cochran & David B. Apatoff, *The Clock is Ticking: Congress Scrambles to Limit Y2K Liability Before Wave of Lawsuits*, LEGAL TIMES, Mar. 8, 1999, at 22, 24.

67. *Id*.

68. *Id*.

69. *See, e.g.*, 18 U.S.C.A. § 286 (West 1999) (pertaining to conspiracy to defraud the government with respect to claims); *Id.* § 287 (pertaining to false, fictitious, or fraudulent claims); *Id.* § 1001 (pertaining to false statements); *see generally* 31 U.S.C.A. §§ 3729-3733 (pertaining to civil false claims).

70. The Deputy Secretary of Defense has stated that there will be no pay problems for DOD military and civilian personnel. *See* Jim Garamone, *Hamre: Y2K won't stop DOD pay*, GOV'T EXECUTIVE, Jan. 20, 1999, *available at* <http://www.govexec.com/dailyfed/0199/012099t1.htm>.

71. Lee Davidson, *Y2K Threatens Chemical Plants*, DESERET NEWS, Mar. 15, 1999, *available at* <http://www.deseretnews.com/dn/view/0,1249,70001583,00.html>.

First, local commanders in the United States may still "undertake immediate, unilateral, emergency response actions that involve measures to save lives, prevent human suffering, or mitigate great property damage, only when time does not permit approval by higher headquarters."[74] Overseas commanders may respond immediately "when time is of the essence and humanitarian considerations require action."[75] Beyond this immediate response authority, commanders may only respond to requests submitted through the Federal Emergency Management Agency (within the United States) or the Department of State (overseas).[76] The DOD has also limited the ability of certain military units with high-priority national security missions to respond to Y2K emergencies in ways that would compromise operational readiness. Finally, the DOD has prioritized the types of emergencies that units will respond to (for example, maintenance of domestic public safety has a higher priority than maintenance of the economy).[77] Judge advocates can and should play an important role in assisting commanders in navigating the myriad of legal authority guiding the assistance rendered.

Conclusion

The Y2K problem is getting more and more coverage in the press as the end of the millennium grows near. Commanders and staff are likely to grow more interested in all aspects of Y2K; to include the legal issues involved with the problem. Judge advocates should begin to take steps to answer that need. Staff judge advocates and command judge advocates should consider appointing an attorney to be the main point of contact for all Y2K legal issues. Different branches of the staff judge advocate's office should plan not only for the effects of Y2K on internal office operations but should also plan for community-wide effects within their areas of responsibility. The Y2K bug may not be the end of the world, but it will undoubtedly cause disruptions, and judge advocates should be prepared to address the legal issues involved. Major Gross.

---

72. Fort Sill and Tinker Air Force Base in Oklahoma both responded to the blast that destroyed the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma on 19 April 1995. *See* Commander Jim Winthrop, *The Oklahoma City Bombing: Immediate Response Authority and Other Military Assistance to Civil Authority (MACA)*, ARMY LAW., Jul. 1997, at 3 (providing a thorough overview of the legal authorities affecting both military support to civil authorities and civilian law enforcement agencies). *See* INTERNATIONAL & OPERATIONAL L. DEP'T, THE JUDGE ADVOCATE GENERAL'S SCHOOL, U.S ARMY, JA-422, OPERATIONAL LAW HANDBOOK, chs. 21, 22 (1997).

73. *See* Memorandum, Deputy Secretary of Defense, to The Secretaries of the Military Departments et al., subject: DOD Year 2000 (Y2K) Support to Civil Authorities (22 Feb. 1999) *available at* <http://www.army.mil/army-y2k/depsecdef_dod_civil_support.htm>.

74. *Id.*

75. *Id.*

76. *Id.*

77. *Id.*